DarkCasino行动：APT组织Evilnum近期攻击事件深入分析

伏影实验室

一、概述

近期，绿盟科技伏影实验室捕获了一系列针对欧洲国家的网络钓鱼活动。这些活动主要针对线上赌博平台，目标为通过攻击此类服务背后的活跃的线上交易行为，窃取服务商和消费者的交易凭据，进而获取非法收益。

通过深入分析，伏影实验室确定该系列活动是APT组织Evilnum近期攻击活动（http://blog.nsfocus.net/agentvxapt-evilnum/）的延续。与既往活动相比，Evilnum攻击者在本次行动中继承了其代表性的攻击手法，但使用了更多样的攻击流程与复杂的攻击组件，并启用了两种新型木马程序DarkMe与PikoloRAT，展现了其较高的工具开发能力、流程设计能力与丰富的攻防对抗经验。同时，因为不同攻击流程的设计思路与具体实现存在明显差异，伏影实验室认为有多个攻击者同时参与了此次行动。

通过提取攻击目标与主要木马程序的关键词并组合，伏影实验室将Evilnum的该起行动命名为DarkCasino。该起行动表明Evilnum仍然以在线交易平台为主要目标，能够迅速发现网络犯罪机会并执行攻击。

截至报告发布时，该DarkCasino行动仍在持续。

二、组织信息

Evilnum是一个在2018年被发现的APT组织，活跃于英国和欧盟国家，主要攻击目标为金融科技公司，目的为通过窃取交易凭证盗取公司或个人账户资金。组织名称Evilnum来自同名的木马程序，亦被卡巴斯基称为DeathStalker。

Evilnum的代表性攻击手段是将恶意程序伪装成客户的身份证明文件，欺骗金融公司的工作人员运行这些程序，进而通过植入间谍木马获得受害者主机上的高价值信息。

Evilnum有较强的开发能力，能够设计复杂的攻击流程和攻击组件。绿盟科技伏影实验室曾捕获和披露该组织具有高完成度的攻击流程和一款stub型木马AgentVX。

三、影响面分析

分析发现，Evilnum本次行动的受害者主要分布于地中海区域的欧洲国家以及加拿大、新加坡、菲律宾等相关国家，其直接攻击目标包括线上赌场平台、使用此类平台的各国消费者以及与平台线上交易行为有关的其他人员。

已发现的攻击流程中，Evilnum使用以下字符串作为诱饵文件名：

诱饵文件名
offer deal visa 2022.lnk
offer crypto casino.scr
Scatters Casino offers Daily Promotions.pif
new casino crypto.com
Promo CPL CPA Traffic.com
PayRedeemUpdateIntegration19052022.scr
DOCUMENTATION AGREEMENTS S CONSULTING INTEGRATION.pif

上述内容中的Scatters Casino是一家由马耳他公司Gammix Limited运营的线上赌场，这些诱饵文件一边尝试将自身伪装为线上交易证明或广告投放服务促销文件以攻击scatters的运营人员，一方面也尝试伪装为scatters促销广告来攻击scatters的用户，从而使Evilnum攻击者能够获取这些目标的主机上保存的交易凭证或相关信息。

对各式诱饵文档的来源进行统计，伏影实验室发现本次DarkCasino活动的受害者广泛分布于马耳他、波兰、塞浦路斯、亚美尼亚、西班牙、瑞士、法国、爱尔兰等欧洲国家，以及加拿大、以色列甚至新加坡、菲律宾等非欧洲国家：

图3.1 DarkCasino行动受害者分布情况

可以发现受害者地理位置以马耳他为核心，辐射至多个可能使用scatters网站服务的国家。

scatters的线上赌场平台成立于2019年，扩张十分迅速。目前，scatters网站声称其线上赌场服务拥有价值2.3亿欧元的奖池，这可能是Evilnum本次行动将其作为目标的主要原因。

此外，一些信息表明，DarkCasino行动有可能是一场规模更大且更持久的网络攻击活动的一部分。IoC关联线索显示，Evilnum的部分资产可以关联至一场从2021年下半年开始延续至2022年年初的，针对加密货币相关交易平台和用户的网络攻击活动。在这场活动中，攻击者主要投递了大量带有签名的ParallaxRAT和NetWire木马，用于窃取目标主机信息，其主要影响目标主要集中在欧洲国家。虽然攻击者在该活动中使用的诱饵形式及网络资源与DarkCasino行动存在一定程度的关联，但伏影实验室尚未获取直接证据证明该活动同样是Evilnum所为，该攻击者可能是以合作的形式借用Evilnum资产并加入其行动中。

四、攻击流程分析

本次行动中，Evilnum组织攻击者主要创建了三类不同的攻击流程。三类流程以不同类型的诱饵文件为起始，通过访问公有资源或失陷站点获取隐写图片，提取其中的DarkMe木马载荷内容后用不同的方式加载执行。

4.1 攻击流程A

这是Evilnum攻击者最早实现的一类攻击流程，同时也是组件复杂度最高的流程。关键组件的最早发现日期为5月2日。

研究不同的组件时发现，该攻击流程包含两种变型，分别为创建时间为4月28日的，从网络位置获取内容的流程A1；以及创建时间为5月1日的，不需要联网下载内容的流程A2。两种变型的实际执行过程相似。

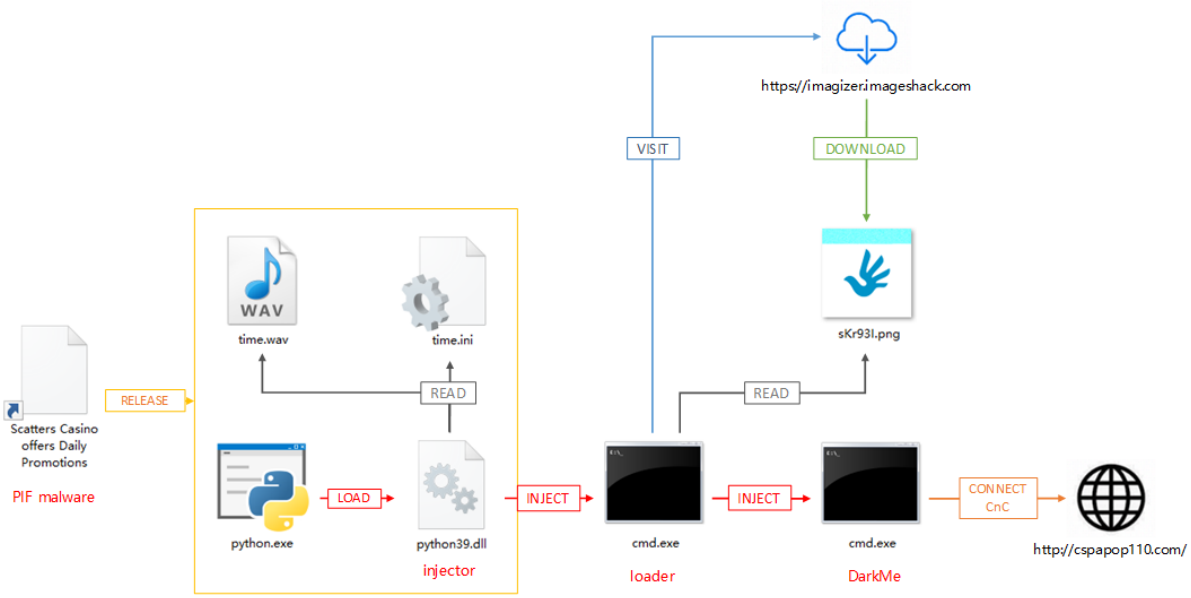

图4.1 DarkCasino攻击流程A

图为流程A1的图示。该流程与伏影实验室稍早披露的Evilnum组织AgentVX攻击活动（http://blog.nsfocus.net/agentvxapt-evilnum/）非常类似，由InstallShield安装程序、侧加载程序、加密ShellcodeLoader、隐写图片以及DarkMe木马程序构成。

伪装成PIF文件的InstallShield程序启动后，会执行安装程序的一般流程，在系统%TEMP%目录下释放内置的文件并运行其中的合法程序python.exe。

python.exe启动后会以侧加载的形式运行携带恶意代码的python39.dll程序，从而启动其中的一段shellcode。

python39.dl中恶意shellcode的功能为读取同目录下的time.wav文件并解密提取其中的下一阶段shellcode代码，随后启动cmd.exe傀儡进程并将下一阶段shellcode分段注入其中，并将从time.ini中读取的一段url地址字符串作为shellcode的启动参数写入cmd.exe傀儡进程中。

cmd.exe傀儡进程中的shellcode会从上述url地址获取一张隐写图片，并通过内置的图像处理模块从图像中提取第三阶段的shellcode并运行。

第三阶段的shellcode会尝试将内置的DarkMe木马注入至另一cmd.exe傀儡进程中运行。该DarkMe木马通信CnC为cspapop110.com。

4.2 攻击流程B

这是最早在5月9日观测到的一类攻击流程，相关文件显示流程的构建时间为5月3日。

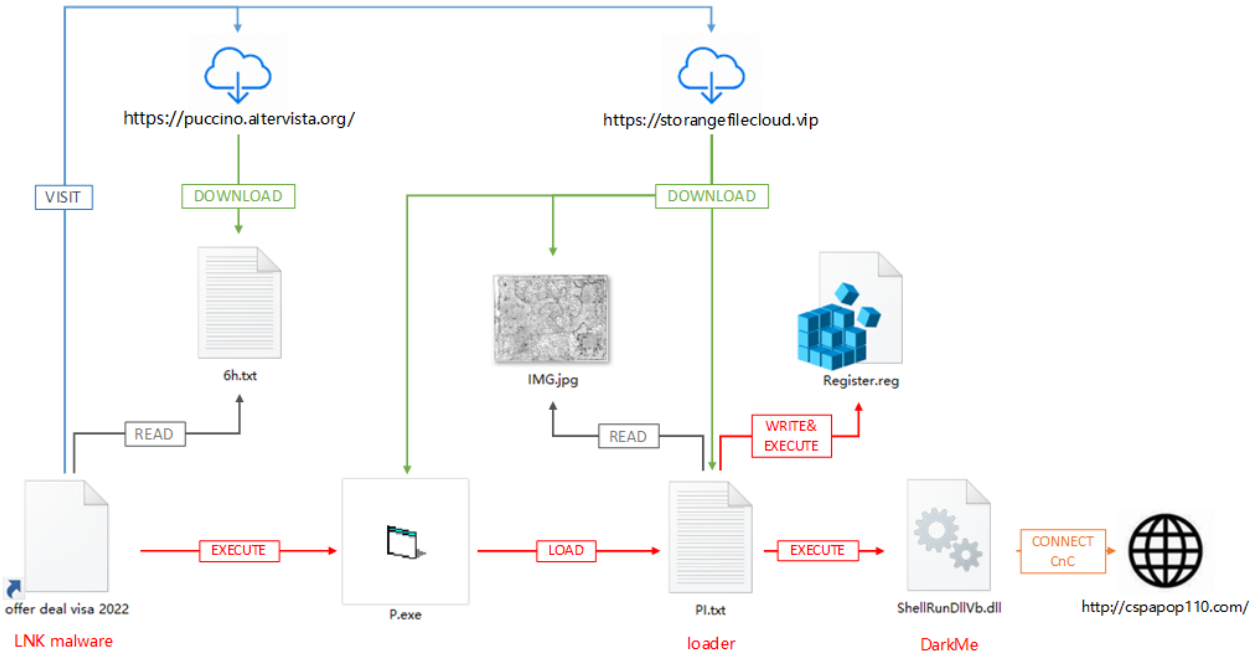

图4.2 DarkCasino攻击流程B

上图为流程B的图示。该过程中，攻击者沿袭了组织的一贯思路，通过投递带有恶意mshta指令的快捷方式诱饵文件，访问受控wordpress站点获取后续的指令代码并运行。

本流程的关键阶段在于通过访问第二阶段站点获取的三个文件P.exe, PI.txt与IMG.jpg。被P.exe加载后，主要loader木马PI.txt会提取IMG.jpg中隐藏的可执行文件ShellRunDllVb.dll，并通过创建名为Register.reg的注册表文件将该dll文件注册为系统组件{A762B0C7-5244-4B3E-ADED-D549E9CEA39E}。loader木马最终通过rundll32 /sta命令执行该组件。

上述操作最终执行的是名为DarkMe的间谍木马程序，通信CnC为cspapop110.com。

4.3 攻击流程C

Evilnum攻击者在5月19日补充了一种更精简的流程。

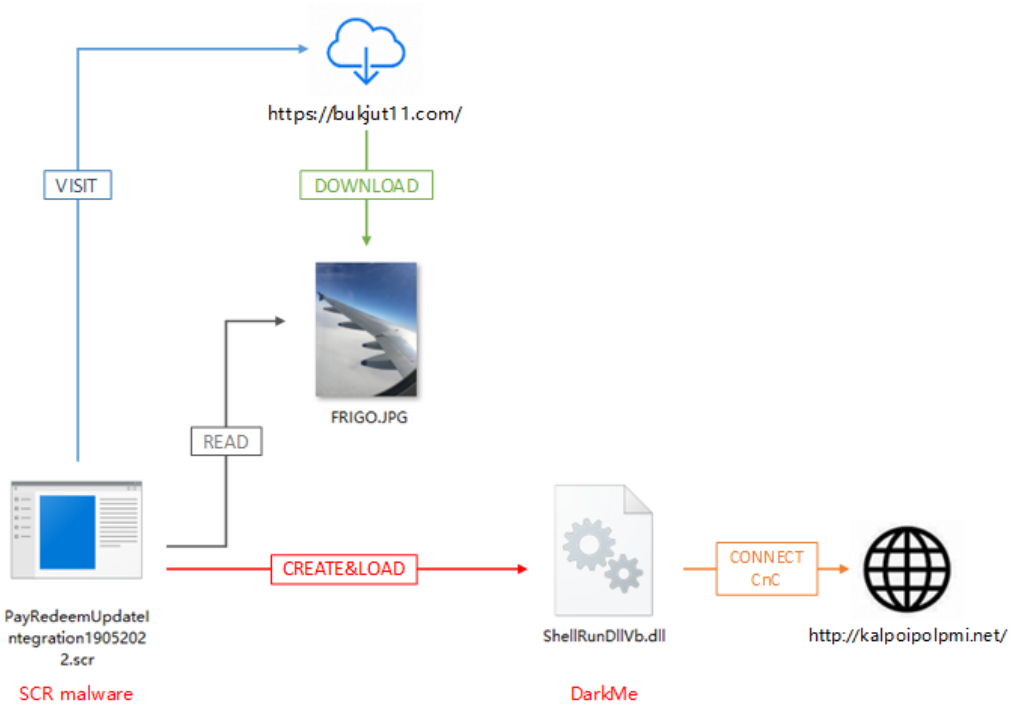

图4.3 DarkCasino攻击流程C

上图为流程C的图示。该流程通过伪装成scr文件的loader木马发起。木马通过直接访问内置的url链接获取一张隐写图像，随后提取其中的ShellRunDllVb.dll文件并加载执行。该dll文件同样是DarkMe木马，通信CnC为kalpoipolpmi.net。

五、组件分析

本次行动中，Evilnum主要使用了一种自制的新型木马程序。伏影实验室通过木马程序中的特殊字符串将其命名为DarkMe。

此外，伏影实验室在进行关联分析时发现了另一种与Evilnum本次行动有紧密联系的新型木马程序，并通过其中特殊字符串将其命名为PikoloRAT。

5.1 DarkMe

DarkMe是一种VisualBasic间谍木马，由Evilnum攻击者开发并运用在各类攻击流程中。DarkMe的初始版本出现在2021年9月25日，至今已迭代出5个版本。

DarkMe的通信能力通过一种公开的WinSock32模块（http://leandroascierto.com/blog/winsock32/）实现。该模块通过创建名为SOCKET_WINDOW的窗口，以窗口信息的方式与服务端进行套接字通信。

DarkMe木马在该模块的基础上陆续添加了大量功能代码，使其从下载者木马逐渐演变成具有间谍软件能力的stub类型木马。

5.1.1 功能

由于不同版本DarkMe的功能代码不同，此处以本次行动中出现的V5版本木马程序（ShellRunDllVb.dll）进行说明。

该木马在运行后首先会采集宿主机信息并发送至CnC。V4版本收集的信息包括宿主机所在地理位置缩写、所在国家全称、计算机名、用户名、反病毒软件列表、木马标记以及前台窗口标题，这些信息使用固定分隔符0x3F分隔，并在前部添加固定字符串"92"，形成上线信息并发送至CnC端。

```
00000000  39 32 3f 3f 3f 43 4e 3f  50 65 6f 70 6c 65 27 73   92???CN? People's
00000010  20 52 65 70 75 62 6c 69  63 20 6f 66 20 43 68 69    Republi c of Chi
00000020  6e 61 3f                                          na?
00000030                          3f  4e 6f 20 41 6e 74 69 76         ? No Antiv
00000040  69 72 75 73 3f 70 61 73  73 77 6f 72 64 3f d5 fd   irus?pas sword?..
00000050  d4 da b2 b6 bb f1 20 b1  be b5 d8 c1 ac bd d3 3f   ...... . .......?
```

图5.1 DarkMe上线流量

DarkMe实现了多个模块，以支持各类间谍功能。其中一个主要模块名为clsfile，用于实现在CnC控制下的文件操作。CnC控制指令由通信内容的前6字节给出，各指令对应操作如下表：

指令	功能
300100	获取磁盘分卷信息
STRFLS	遍历指定目录获取目录结构
STRFL2	遍历指定目录获取目录结构，支持大型目录
SHLEXE	执行cmd命令
RNMFIL	重命名指定文件
DELDEL	删除指定文件
DIRMAP	创建指定目录
DELMAP	删除指定目录
SEITUS	写入指定文件
SEITUD	读取指定文件
ZIPALO	写入压缩文件
FRIKAT	写入注册表启动项
COPALO	复制指定文件
PASALO	粘贴指定文件

表5.1 DarkMe指令对照表

此外，DarkMe还融合了一套公开代码（https://forums.codeguru.com/showthread.php?15579-Save-Screen-Capture-output-to-a-file），实现了屏幕截图功能。

```
' Depending on the value of Client get the proper device context.
If Client Then
hDCSrc = GetDC(hWndSrc) ' Get device context for client area.
Else
hDCSrc = GetWindowDC(hWndSrc) ' Get device context for entire
' window.
End If

' Create a memory device context for the copy process.
hDCMemory = CreateCompatibleDC(hDCSrc)
' Create a bitmap and place it in the memory DC.
hBmp = CreateCompatibleBitmap(hDCSrc, WidthSrc, HeightSrc)
hBmpPrev = SelectObject(hDCMemory, hBmp)

' Get screen properties.
RasterCapsScrn = GetDeviceCaps(hDCSrc, RASTERCAPS) ' Raster
' capabilities.
HasPaletteScrn = RasterCapsScrn And RC_PALETTE ' Palette
' support.
PaletteSizeScrn = GetDeviceCaps(hDCSrc, SIZEPALETTE) ' Size of
' palette.

' If the screen has a palette make a copy and realize it.
If HasPaletteScrn And (PaletteSizeScrn = 256) Then
' Create a copy of the system palette.
LogPal.palVersion = &H300
LogPal.palNumEntries = 256
r = GetSystemPaletteEntries(hDCSrc, 0, 256, _
LogPal.palPalEntry(0))
hPal = CreatePalette(LogPal)
' Select the new palette into the memory DC and realize it.
hPalPrev = SelectPalette(hDCMemory, hPal, 0)
r = RealizePalette(hDCMemory)
End If
```

```
75
76  Private  Proc_3_2_11014A40_CaptureWindow(arg_C, arg_10, arg_14, arg_18
    , arg_1C) '11014A40
77    Dim var_43C As var_18)
78    loc_11014A62: var_8 = ""
79    loc_11014A6C: edx = ""
80    loc_11014A73: eax = ""
81    loc_11014A7F: var_14 = ""
82    loc_11014A84: var_430 = ""
83    loc_11014A8A: var_43C = ""
84    loc_11014A90: If arg_C = 0 Then GoTo loc_11014A9D
85    loc_11014A96: var_8004 = GetDC(Me)
86    loc_11014A9B: GoTo loc_11014AA6
87    loc_11014A9D: ' Referenced from: 11014A90
88    loc_11014AA1: var_8008 = GetWindowDC(Me)
89    loc_11014AA6: ' Referenced from: 11014A9B
90    loc_11014AAE: var_800C = GetLastError
91    loc_11014AB1: var_8010 = CreateCompatibleDC(var_8008)
92    loc_11014AB8: var_8014 = GetLastError
93    loc_11014AC3: var_8018 = CreateCompatibleBitmap(var_8008, arg_18,
      arg_1C)
94    loc_11014AC8: var_444 = var_8018
95    loc_11014ACE: var_801C = GetLastError
96    loc_11014AD8: var_8020 = SelectObject(var_8010, var_444)
97    loc_11014ADD: var_444 = var_8020
98    loc_11014AE3: var_8024 = GetLastError
99    loc_11014AEE: var_440 = var_444
100   loc_11014AF4: var_8028 = GetDeviceCaps(var_8008, 38)
101   loc_11014AF9: var_444 = var_8028
```

图5.2 DarkMe截图功能（右）与公开实现（左）

DarkMe的其他功能还包括持久化、自更新，以及部分版本中出现的键盘记录。

5.1.2 版本

通过挖掘在野样本，伏影实验室发现DarkMe木马已有半年以上的发展历史，并产生多个版本。该木马的版本迭代时间线如下：

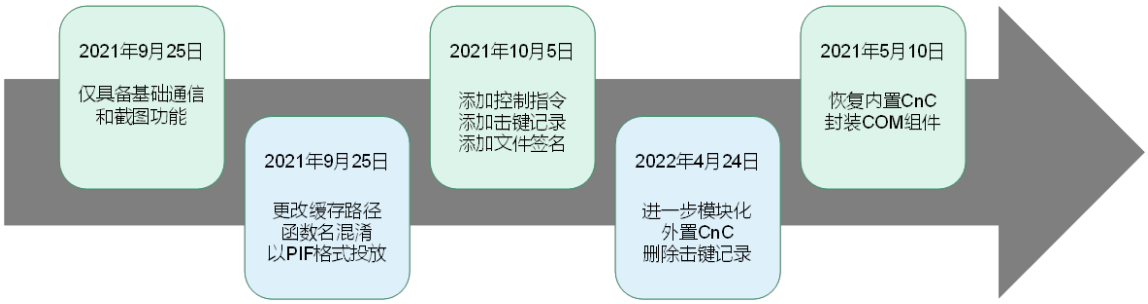

图5.3 DarkMe版本迭代过程

可以看到，在其生命周期内，DarkMe木马的定位发生了变化，从直接投放的loader型木马程序发展为间谍木马程序，进而发展为融入复杂攻击流程中的stub载荷。代码功能完善的V4与V5版本DarkMe木马既可以作为基本的窃密工具使用，也可以作为其他工具的装载器使用，因此被Evilnum攻击者广泛应用于近期攻击行动中。

5.2 PikoloRAT

通过对本次活动的关联信息进行深入挖掘，伏影实验室发现了另一种新型远程控制木马PikoloRAT。该木马带有典型的远程控制功能，并可以使用内置组件开展更复杂的控制操作。

由于已发现的PikoloRAT木马内置CnC地址与本次Evilnum行动中使用的地址重合，并且其功能可以与上述DarkMe木马形成互补，因此伏影实验室判断，PikoloRAT是由Evilnum攻击者在入侵后期阶段使用的扩展组件。

已发现的案例中，PikoloRAT通过一种下载者木马投放，或包装为压缩文件投放。

5.2.1 功能

PikoloRAT是一种使用C#编写的典型RAT木马程序。

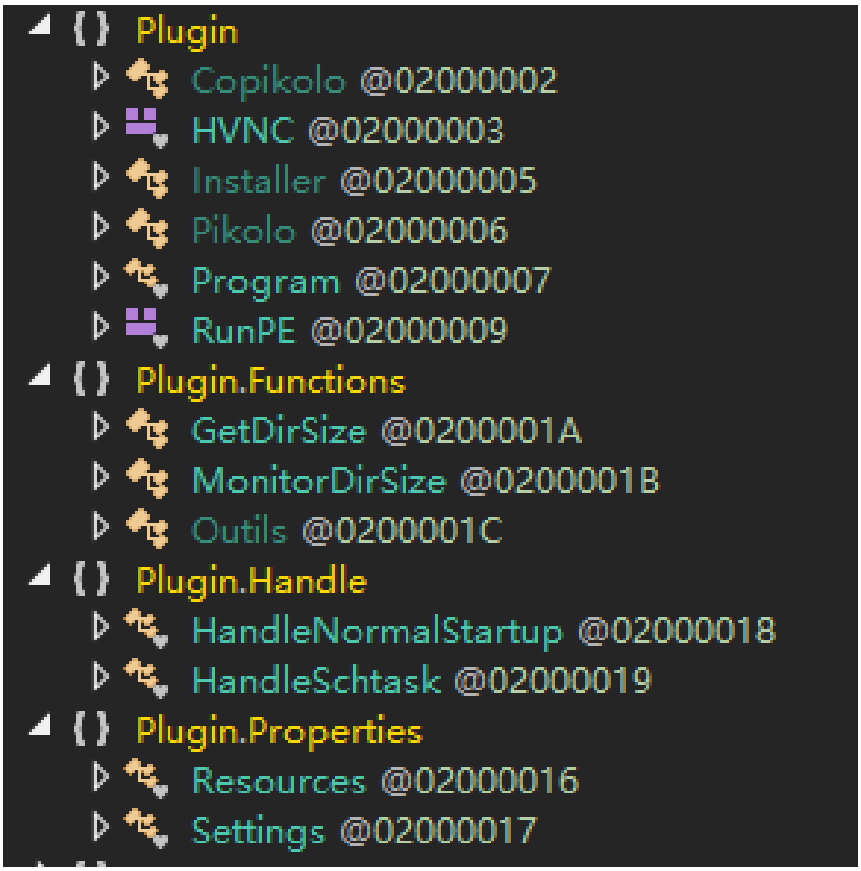

图5.4 PikoloRAT主体框架

木马运行后首先会收集宿主机信息并上传，收集内容包括木马标记、用户名、计算机名、所在地理位置、操作系统版本、木马运行时间、木马版本、反病毒软件信息。木马使用分隔符"|"分隔这些信息，并在前部添加固定字符串"654321"，并发送给CnC。

```
00000000  67 00 00 00 00 00 00 00                           g.......
00000008  00 01 00 00 00 ff ff ff  ff 01 00 00 00 00 00 00  ........ ........
00000018  00 06 01 00 00 00 4f 36  35 34 33 32 31 7c 43 2b  ......O6 54321|C+
00000028  2b 7c                                             +|
00000038                                    7c 55 53 7c 57           |US|W
00000048  69 6e 64 6f 77 73 20 37  20 55 6c 74 69 6d 61 74  indows 7  Ultimat
00000058  65 7c 30 35 2f 32 34 2f  32 30 32 32 7c 33 2e 30  e|05/24/ 2022|3.0
00000068  7c 54 72 75 65 7c 0b                              |True|.
```

图5.5 PikoloRAT上线流量

可以看到，该信息内容与格式与上述DarkMe木马类似。

随后，PikoloRAT进入受控状态，通过获取CnC端指令控制宿主机行为。其支持的远控操作指令如下表：

指令码	操作
1	退出指令循环
2	左键单击按下
3	右键单击按下
4	左键单击抬起
5	右键单击抬起
6	左键双击
7	按下对应键盘按键
8	鼠标移动到指定位置
9	获取剪贴板内容
17	设置屏幕截图间隔
18	设置屏幕截图质量
19	设置屏幕截图缩放尺寸
24	结束自身进程
55	设置临时文件路径
4875	执行cmd命令
4876	执行powershell命令
8888	加载运行PEGASUS HVNC
8889	卸载木马本体
8890	持久化，包括添加自启动项和计划任务
8891	删除持久化内容

表5.2 PikoloRAT指令对照表

可以看到除基本的远控功能外，PikoloRAT还可以通过释放内置的PEGASUS HVNC模块（一种近期泄露的hVNC工具）执行更完善的远程控制。

六、技战术分析

6.1 覆写式侧加载

本次攻击流程A中，Evilnum攻击者投递了一个恶意的python39.dll文件，并通过合法文件python.exe侧加载该恶意文件。

与常见侧加载构建逻辑不同的是，该恶意python39.dll实际上是通过直接覆写原始python39.dll文件得到的。Evilnum攻击者将一段shellcode直接写入原始python39.dll的函数PyImport_AddModuleObject的位置，使python39.dll在被加载时自动启动该shellcode。

该设计的好处在于：

操作简便，无需编译独立的dll程序并实现其导出方法；

适用性广，理论上可以对任意合法dll文件进行类似的覆写操作，构建侧加载shellcode攻击链；

隐蔽性强，覆写后dll文件与原始dll文件相似度很高，不易被定位。

```
.text:1023DA30 ; FUNCTION CHUNK AT .text:1023E997 SIZE 00001CFB BYTES
.text:1023DA30
.text:1023DA30                 push    ebp
.text:1023DA31                 mov     ebp, esp
.text:1023DA33                 sub     esp, 978h
.text:1023DA39                 mov     [ebp+var_1FC], 1B3h
.text:1023DA43                 mov     [ebp+var_1], 0B2h
.text:1023DA47                 mov     eax, 0C0h
.text:1023DA4C                 mov     [ebp+var_3E4], ax
.text:1023DA4C                                         ; CODE XREF: sub_10252510+92↓p
.text:1023DA4C                                         ; sub_10255D10+D↓p ...
.text:1023DA53                 mov     [ebp+var_720], 70h ; 'p'
.text:1023DA5D                 mov     [ebp+var_71C], 10DCE133h
.text:1023DA67                 mov     [ebp+var_718], 4Ch ; 'L'
.text:1023DA71                 mov     [ebp+var_714], 48h ; 'H'
.text:1023DA7B                 mov     [ebp+var_710], 2Ch ; ','
.text:1023DA85                 mov     [ebp+var_70C], 7Eh ; '~'
.text:1023DA8F                 mov     [ebp+var_D4], 124h
.text:1023DA99                 mov     [ebp+var_5D8], 15h
.text:1023DAA3                 mov     [ebp+var_5D4], 850F70h
```

图6.1 python39.dll中被覆写的PyImport_AddModuleObject函数

6.2 Shellcode框架

本次攻击流程A中，Evilnum攻击者在不同阶段使用了多种shellcode。这些shellcode具有类似的代码实现逻辑，可以看出来自相同的shellcode编程框架，整体构成与代码复杂度相较既往Evilnum活动有所提升。

6.2.1 ntdll映射

本次行动出现的shellcode中，攻击者依然坚持使用kernel32与ntdll两个模块构建主体流程。为了规避针对此类行为的api检测思路，攻击者使用如下的方式映射ntdll文件并使用映射文件的api：

```
vGetSystemDirectoryW = (void (__cdecl *)(__int16 *, int))getprocaddr_D428(vbasekernel32, 0x72641C0B);
vGetSystemDirectoryW(vpsysdir, v399);
v565[0] = 'n';
v565[1] = 't';
v565[2] = 'd';
v565[3] = 'l';
v565[4] = 'l';
v565[5] = '.';
v565[6] = 'd';
v565[7] = 'l';
v565[8] = 'l';
v565[9] = 0;
strcat_D0F8((int)vpsysdir, (int)v565);
vmappedbase = genfilemapping_D4C8((int)vpsysdir, vbasekernel32);
vGlobalAlloc = (int (__cdecl *)(int, int))getprocaddr_D428(vbasekernel32, 0x7FBC7431);
vNtAllocateVirtualMemory = (int (__cdecl *)(int, int *, _DWORD, int *, int, int))getprocaddr_D428(
                                                                                    vbasentdll,
                                                                                    0xD820A574);
vmappedNtAllocateVirtualMemory = calcmappingpadding_D5D8((int)vNtAllocateVirtualMemory, vbasentdll, vmappedbase);
```

图6.2 Shellcode中的ntdll模块映射逻辑

该实现中，攻击者通过文件映射的方式重新加载ntdll模块，并在获取原始ntdll中api基址后通过计算偏移的方式记录映射模块中对应的api基址。shellcode在后续的关键过程中，使用映射api实现对应行为，以此避免api调用行为及关键参数被监控记录。

6.2.2 X64call

本次攻击流程A中，攻击者在注入cmd.exe的操作中使用了X64call的方式调用关键API。

注入部分的shellcode首先检测进程环境与主机cpu型号，如满足需求，则在使用NtAllocateVirtualMemory、NtWriteVirtualMemory等关键注入api时调用其64位实现：

```
seg000:000035A5                 jz      short loc_135BF ; if isX64env
seg000:000035A7                 push    5
seg000:000035A9                 pop     edi
seg000:000035AA                 push    edi
seg000:000035AB                 lea     eax, [ebp+vvhandle]
seg000:000035B1                 push    eax
seg000:000035B2                 push    [ebp+var_20]
seg000:000035B5                 call    near ptr X64call_11E00
seg000:000035BA                 add     esp, 0Ch
seg000:000035BD                 jmp     short loc_135D2
seg000:000035BF ; ---------------------------------------------------------------------------
seg000:000035BF
seg000:000035BF loc_135BF:                              ; CODE XREF: sub_12A09+B9C↑j
seg000:000035BF                 lea     eax, [ebp+var_160] ; else
seg000:000035C5                 push    eax
seg000:000035C6                 push    ecx
seg000:000035C7                 push    edi
seg000:000035C8                 push    ebx
seg000:000035C9                 push    [ebp+vhandle]
seg000:000035CC                 call    [ebp+vNtWriteVirtualMemory]
seg000:000035CF                 push    5
seg000:000035D1                 pop     edi
```

图6.3 Shellcode注入代码中的X64call调用逻辑

```
seg000:00001EAE                 push    ebx
seg000:00001EAF                 push    esi
seg000:00001EB0                 push    edi
seg000:00001EB1                 mov     [ebp+var_4], esp
seg000:00001EB4                 and     esp, 0FFFFFFF0h
seg000:00001EB7                 push    33h ; '3'
seg000:00001EB9                 call    $+5
seg000:00001EBE                 add     [esp+58h+var_58], 5
seg000:00001EC2                 retf
```

图6.4 X64call调用代码

这种技巧同样可以起到规避api检测的效果。

6.3 图片隐写

本次行动中，Evilnum攻击者使用了两种形式的隐写图片。

流程B中，名为IMG.jpg的图片使用了冗余隐写，将恶意代码存放于文件尾部，使用固定字符串(HEHE)作为分隔标志：

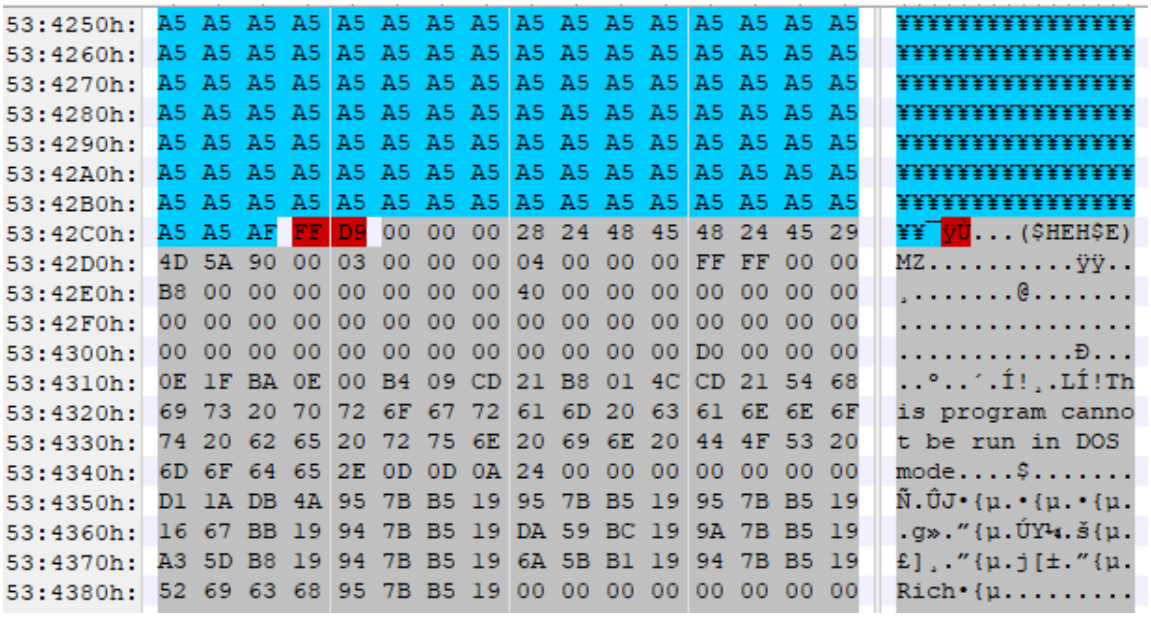

图6.5 IMG.jpg中的隐写信息

流程A中，携带载荷的图片则使用了RGB值隐写，将恶意代码存放于RGB值的R位：

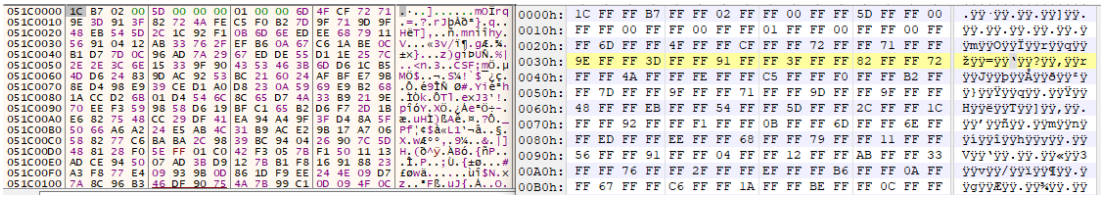

图6.6 隐写图片sKr93l.png中的RGB值（右）与提取到的压缩数据内容（左）

这样的构造使隐写图片在白色区域显示蓝绿色斑点，黑色区域则显示红色斑点：

图6.7 隐写图片sKr93l.png外观

图6.8 隐写图片Fruit.png外观

6.4 套接字窗口

本次DarkCasino行动中，Evilnum使用的DarkMe木马使用了SOCKET_WINDOW通信。

这是一种古老的VisualBasic套接字编程技术，通过一个SOCKET_WINDOW窗口挂钩winsock消息，并在窗口回调函数中处理由WSAAsyncSelect传递的事件消息。

原始框架可参考：https://github.com/dzzie/RE_Plugins/blob/master/IdaVbScript/vb%20src/MSocketSupport.bas

6.5 COM组件执行

本次DarkCasino行动中，部分DarkMe木马以COM组件的形式投递。Evilnum攻击者在前置木马载荷中写入注册表操作逻辑，使其可以产生并执行带有如下内容的Register.reg文件：

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B0C7-5244-4B3E-ADED-D549E9CEA39E}]
@="ShellRunDllVb.CShellRunDll"
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B0C7-5244-4B3E-ADED-D549E9CEA39E}\Implemented Categories]
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B0C7-5244-4B3E-ADED-D549E9CEA39E}\Implemented Categories\
{40FC6ED5-2438-11CF-A3DB-080036F12502}]
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B0C7-5244-4B3E-ADED-D549E9CEA39E}\InprocServer32]
@="C:\\Users\\          \\AppData\\Local\\Update\\ShellRunDllVb.dll"
"ThreadingModel"="Apartment"
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B0C7-5244-4B3E-ADED-D549E9CEA39E}\ProgID]
@="ShellRunDllVb.CShellRunDll"
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B0C7-5244-4B3E-ADED-D549E9CEA39E}\Programmable]
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B0C7-5244-4B3E-ADED-D549E9CEA39E}\TypeLib]
@="{8F1576C0-BB08-4F05-87A6-268C0D548794}"
[HKEY_CURRENT_USER\Software\Classes\CLSID\{A762B0C7-5244-4B3E-ADED-D549E9CEA39E}\VERSION]
@="1.0"
```

图6.9 Register.reg文件内容

随后前置木马载荷通过形如rundll /sta [CLSID] 'Hello'的cmd指令启动DarkMe木马。

这样的方式避免了对DarkMe木马的直接调用，一定程度上减少了暴露风险。

七、总结

DarkCasino行动是一场正在发生的，针对网络交易现金流的APT攻击活动。Evilnum在该行动中使用了多种经过不断改良的攻击手法和工具，展现了其敏锐的对抗意识。

分析表明， DarkCasino行动的影响范围并不局限于欧洲，在Evilnum攻击者的运营下，本次攻击最终辐射到了部分亚洲国家，有可能造成意料之外的危害。

为有效防范本次APT行动，应尤其注意通过各种渠道传递的LNK、PIF、SCR、COM类型文件，提高对带有offer、visa、casino等关键词的文件的警觉性，避免因Evilnum的网络攻击造成直接经济损失。

八、IoCs

攻击流程A诱饵文件

43eda4ff53eef4513716a5b773e6798653ee29544b44a9ae16aa7af160a996f2	offer deal visa 2022.lnk

攻击流程B诱饵文件

5fb252474237a4ca96cc0433451c7d7a847732305d95ceeaeb10693ecef2eeee	Scatters Casino offers Daily Promotions.pif
8e4a4c5e04ff7ebacb5fe8ff6b27129c13e91a1acc829dbb3001110c84dc8633	new casino crypto.com
d0899cb4b94e66cb8623e823887d87aa7561db0e9cf4028ae3f46a7b599692b9	Promo CPL CPA Traffic.com

攻击流程C诱饵文件

4ffa29dead7f6f7752f2f3b0a83f936f270826d2711a599233dc97e442dee85f	333TER.exe
9cf7f8a93c409dd61d019ca92d8bc43cc9949e244c9080feba5bfc7aac673ac3	d33v3TER.exe
259cebed2cd89da395df2a3588fadde82cd6542bc9ff456890f7ee2087dc43c9	d333TER.exe
0cdf27bb8c0c90fc1d60fb07bd30b7e97b16d15e3f58fb985350091ecad51ba6	ed333TER.exe
5ba84191a873d823ccf336adfa219cc191a004e22b56b99c6d0e1642144129b8	wed333TER.exe
15a076c7bb6a38425d96aa08b8a15e9a838c9697d57c835aaca92fd01607b07a	PayRedeemUpdateIntegration190520
3329f5e3a67d13bd602dca5bbe8e2d0b5d3b5cb7cb308965fb2599a66668c207	offer crypto casino.scr
8a49a7f6c95fade72ef86455794cdedfca9129aa0f5281e09929dfebfb3417c4	DOCUMENTATION AGREEMENTS S CONSULTING INTEGRATION.pif

下载者木马

864dccbeda7d88cad91336b5ae9efd50972508d1d8044226e798d039a0bc1da2	AONNRJP.exe

PikoloRAT木马

eb5e42c726c7b125564455d56a02b9d42672ca061575ff911672b9165e8e309d	stub1.exe
be544a1f9f642bb35a9bd0942ae16a7a6e58a323d298a408a00fa4c948e8ea17	Stub1.exe

DarkMe木马

a826570f878def28b027f6e6b2fcd8be1727e82666f8b65175d917144f5d0569	Project1.exe
7b478cd8b854c9046f45f32616e1b0cbdc9436fa078ceddb13ce9891b24b30a5	Project1.exe
e72337c08d6b884b64fd9945c5a01557ccf40db93af866c00c48d36b6605f3a0	Project1.exe
414a11e8eabb64add97a866502edcd7e54108bd247f4ae12fe07feeae4e549f6	Projec3.exe
7913cdf40cc17a28487a71ab0d7724b8bf3646a2a53e3905798ce23a657061b8	Project1.exe
3a6694567e9d722357b8e92153d9c878bbcab55a2f65cd0f9a2e6579fbeb935a	Projec3.exe
a6a70c85b8c40932678c413fde202a55fcfc9d9cae23822708be5f28f9d5b6d2	Projec3.exe
c50ebe13972e6e378248d80d53478d8e01e754c5d87113d9b6f93bf3b84380b4	Project1.exe
1ac7715b1762788b5dc1f5f2fc35243a072fe77053df46101ce05413cca62666	Projec3.exe
4ecc2925cfb073323314611a3892d476a58ff2f6b510b434996686e2f0ac3af7	Projec3.exe
541b3011953a3ce1a3a4a22c8c4f58c6a01df786a7cc10858649f8f70ee0a2f3	Projec3.exe
f25cbc53d0cc14b715ee83e51946d5793e4e86e71e96f68e9b6c839b514e8cb8	Projec3.exe
4244f274a12f4672f2dda1190559d96c5a9631c9ee573b853c89e30701819b63	Projec24.pif
1f0d908c677fb3ec5b9422eb5f7d2a2b3ffa01659521afc07cc4dfaea27aa532	Nuovo.pif
028057e54a2e813787a14b7d33e6a2caa91485ed879ef1bbcb94df0e1cf91356	bvo.exe
0a9c183f0b5a225228da5e8589fac8b3affe2e51c790a08148ef72481de610c4	bvo.exe
3eb84676249cb26dd3d1962cfca2a9fde442d0feaa1b0351f6331313f3ac1138	bvo.exe

46fbfc263959084d03bd72c5b6ee643711f79f7d76b391d4a81f95b2d111b44e	bvofinal.pif
5e04dd49b82320eca63b483e87453d2a68a9f4873f47d37e5080d537bc811d0e	pppppesst.exe
dc8190279dcea4f9a36208ba48b14e6c8313ef061252027ef8110b2d0bd84640	pppppesst.exe
4959cdba7edee68b5116cc1b8ef5016978d3dff2016f027a4f76b080b7c3849a	faster.exe
24ace8fd73b2a5a13f3e5b459f0764dd4b5bda2cea2b0e13bbf88a88afe0cdac	fastest.exe
c66e6ee55e9799a8a32b7a2c836c26bb7ebea98d09c1535ad9ae59e9628835fb	fastest.exe
32ce8d0dcbfcc2517480d0e08f8896ab4f6ea13ccb0eefe7205cd352c7b359c3	h5a.exe
c192684d296ea587e93457d060cbef900143cf1a11301e6c2e34e264e3e55ef6	h5a.exe
1d01b143a56eba431387b9b973790d174deb48c2e3445d96b131a7d8e0a9d4ef	vvt1.exe
b8ba2c0478649dc099d0a869755a7e205173a9b0d15fad920317a89d07eaa930	vvt1.exe
d95853e6e16d90c00fd72aaeaca9885b953dae14d7d6aa7fedcc6150fb788667	656.exe
7add6700c6e1aa1ac8782fdd26a11283d513302c672e3d62f787572d8ad97a21	ShellRunDllVb.dll
17fe047b9a3695d4fd8ad9d2f7f37486c0bc85db0f9770471442d31410ff26a1	ShellRunDllVb.dll
2665a09ec5b4ca913f9f3185df62495f13611831dba9073779a36df088db143b	ShellRunDllVb.dll
7c06a03d712be8c0df410bea5d1c2004c6247bcde5a46ce51746f18de9621ac1	ShellRunDllVb.dll

URL

https[:]//puccino.altervista.org/wp-content/uploads/2022/05/6h.txt
https[:]//storangefilecloud.vip/IMG.jpg
https[:]//storangefilecloud.vip/PI.txt
https[:]//storangefilecloud.vip/PRGx.jpg
https[:]//bukjut11.com/FRIGO.JPG
https[:]//bukjut11.com:443/AEVC.JPG
https[:]//imagizer.imageshack.com/img922/1527/sKr93I.png
https[:]//imagizer.imageshack.com/img923/7651/jMwIGI.png
https[:]//i.imgur.com/fkNiY9Z.png
https[:]//laurentprotector.com/LRGBPFV.bin
https[:]//laurentprotector.com/NnQFqsOEUtkezvIEcLpfa.bin

Darkme CnC

aka7newmalp23.com
csmmmsp099q.com
muasaashishaj.com
cspapop110.com
938jss.com
8as1s2.com
kalpoipolpmi.net
pallomnareraebrazo.com
185.236.231.74

PikoloRAT CnC

51.195.57.232